Data Governance Case Studies

Lindsey Chenault

MSDS 485 — Data Governance, Ethics, and Law

Philip M. Goldfeder, PhD

27 April 2025

Case Study #1

Eichensehr, Kristen E., ed. 2021. *Contemporary Practice of the United States Relating to International Law.* The American Journal of International Law 115 (2): 309–317. https://doi.org/10.1017/ajil.2021.10.

The data for this study include sources like press releases from the FBI, CISA, the Department of Justice, and the Office of the Director of National Intelligence (ODNI), as well as declassified intelligence assessments and statements by senior officials. Additionally, cybersecurity firms such as Microsoft and FireEye, as well as respected media organizations like The New York Times, The Washington Post, and Politico, provided supplementary reporting (Eichensehr 2021). The authors clearly cite these sources throughout the text and depend heavily on official documentation and firsthand reports rather than conducting original data collection. Overall, the scope of sources and consistent cross-referencing exhibit that the analysis is adequate and well-supported.

Foreign election interference exposes crucial gaps in the U.S. data governance framework. At the legal level, agencies defend the digital infrastructure that supports free and fair elections; however, fragmented oversight often leaves gaps that sophisticated actors can exploit (Eichensehr 2021). Ethically, government and tech companies face a growing obligation to act as stewards of voter trust by combating disinformation and promoting transparency, which will promote data integrity. Addressing data governance aligns with the broader need for principles that guarantee accountability, auditability, and cross-functional communication (Ishikawa and Rao, 2021).

In this case, there is a clear cybersecurity problem and a need for accountability, active threat detection, and cross-sector coordination. While the study does not highlight any specific legislation exactly, it does emphasize a montage of executive actions, including public threat briefings from the ODNI, targeted sanctions by the U.S. Treasury Department, and proactive disruptions by companies like Facebook and Microsoft (Eichensehr 2021).

Without legislation highlighted in this case, there is an apparent weakness in how the United States approaches election security. Enacting new laws would strengthen democratic discourse by impeding the spread of disinformation, which includes AI-generated content and foreign-backed political messaging. Although the authors demonstrate that cross-sector collaboration and rapid-response efforts have made a meaningful impact, they also argue that these measures remain inconsistent and vulnerable to political interference without the foundation of law. Codifying such practices into legislation would establish long-term stability, reinforce accountability, and help rebuild public trust in the electoral process. Although the U.S. made the best attempt to defend the 2020 election from foreign interference, the overall response was still fragmented and heavily reliant on executive action and private-sector cooperation. The authors illustrate how agencies like the FBI and ODNI collaborated with Microsoft, Facebook, and Twitter to disrupt foreign influence campaigns and secure election infrastructure (Eichensehr 2021). Cyber operations, sanctions, and coordinated takedowns were all vital in protecting the technical integrity of the election and pushing back against disinformation campaigns led by countries like Russia and Iran.

The authors suggest that transparency and cross-sector collaboration were key to the relative success of the 2020 election response. Even so, the authors emphasize that existing solutions have apparent limitations. Dependence on voluntary efforts by private companies and short-term executive actions leaves major gaps in long-term governance. The continued success of efforts to manipulate public opinion highlights how current strategies fall short of fully safeguarding democratic processes in the digital era. Additional solutions should include the passage of federal legislation establishing mandatory cybersecurity protocols for election systems, formalized data-sharing frameworks between government and tech companies, and enhanced penalties for actors (foreign or domestic) who engage in election interference (Chapple 2021). Expanding public digital literacy programs could also play an influential part in helping voters recognize and resist manipulation. In addition, establishing an independent body to oversee election data would lead to more consistent enforcement and greater stability from one election cycle to the next. Together, these steps would help shift the U.S. approach from reactive crisis management toward a more proactive and sustainable model for securing elections.

Case Study #2

The Wall Street Journal. 2019. "How China Is Using Artificial Intelligence in Classrooms." YouTube Video, 7:46. August 2, 2019. https://youtu.be/JMLsHI8aV0g?si=tXR5sLtXXP8HOXvF.

The video titled "How China Is Using Artificial Intelligence in Classrooms" by The Wall Street Journal investigates AI tools like facial recognition cameras and brainwave monitors in Chinese schools. The data for this case study emanate from classroom footage, interviews with students, teachers, and administrators, as well as demonstrations of using the AI systems. While the video presents compelling visual evidence of how the technology is applied, it does not explicitly reference academic studies or technical documentation. The data collection relies on journalistic investigation rather than empirical research. The authors did not disclose details of the AI models or how the data was evaluated. From a media perspective, the data are adequate. Nevertheless, from a research standpoint, The depth of analysis is shallow due to the lack of transparency and scientific validation, which makes it difficult to assess the efficacy or reliability of the AI tools (Zuboff 2019; Hao 2019).

Ethically, deploying AI technologies in classrooms to monitor facial expressions and brain activity obviously makes one worry about student privacy, autonomy, and potential psychological effects. Children, especially, are vulnerable and may not fully understand why or how their biometric data is being collected, processed, or repurposed. Legally, regarding data ownership, storage duration, third-party access, and regulatory compliance, particularly within China's relatively permissive data protection environment, are a concern (Greenleaf and

Livingston 2022). Regarding management, educational institutions must determine how to implement and oversee these systems in a responsible manner. These overlapping issues stress the pressing demand for data governance frameworks that foster transparency, enforce accountability, and require informed consent within AI-driven educational environments (Cummings and Ferris, 2020).

The video does not explicitly address legislation, which leads us to ask a few questions. Are national policies in place to protect students' biometric data, uphold informed consent, and ensure accountability in educational data governance? Effective laws must mandate informed consent, ideally from both students and their guardians, and clearly define the boundaries of data collection, retention, and usage. Regulations should prohibit the repurposing of student data for commercial, disciplinary, or state surveillance purposes. They should include provisions for third-party audits of AI tools to evaluate accuracy, bias, and potential harm (Morley et al., 2020). Without enforceable legislation, the video implicitly advocates for public awareness and critical scrutiny by documenting the perspectives of students and educators. Ultimately, the case study underscores the need for comprehensive oversight through national legislation, school-level policies, or international human rights standards to protect student autonomy and privacy in an increasingly algorithm-driven educational environment.

My primary takeaway from this case study is that while artificial intelligence technologies are being adopted in Chinese classrooms to boost student engagement and academic performance, implementing this technology introduces serious ethical and privacy troubles. The video compellingly illustrates how these tools have become embedded in daily school routines. Yet, it also reveals a troubling lack of transparency regarding consent, data handling, and the potential psychological impact on students. Normalizing surveillance in educational settings,

especially among children who may lack the agency or understanding to question it, poses serious long-term risks to individual autonomy and trust in academic institutions (Zuboff 2019).

The authors do not explicitly propose a solution, which accentuates the severity of the issue: there appears to be little formal oversight or regulatory infrastructure governing these practices. Without clear legal or ethical safeguards, schools may adopt AI tools, assuming that they serve students' best interests without fully accounting for the potential risks. However, in the absence of accountability mechanisms, these interventions risk undermining students' mental health, dignity, and fundamental rights.

Drawing on principles discussed in this course, it is clear that stronger protections are essential. Governments must enact legislation that clearly defines permissible data collection practices in educational settings, limits data retention periods, and requires informed consent from both students and their guardians. Additionally, schools should adopt internal data governance frameworks that require transparency about how data is used, incorporate third-party audits, and include psychological assessments to monitor the impact of surveillance tools (Cummings and Ferris, 2020). Ultimately, AI should be leveraged to support learning outcomes rather than imposing behavioral control. A commitment to ethical integrity, student well-being, and human rights must guide any implementation.

References

Chapple, Michael. 2021. “Why Your Master Data Management Needs Data Governance.” Precisely. April 5, 2021. https://www.precisely.com/blog/datagovernance/why-your-master-data-management-needs-data-governance.

Cummings, Clare, and Madeleine Ferris. 2020. *AI and Data Use in Schools: Balancing Innovation and Child Rights.* UNICEF Office of Global Insight and Policy. https://www.unicef.org/globalinsight/reports/ai-and-data-use-schools.

Eichensehr, Kristen E., ed. 2021. “Contemporary Practice of the United States Relating to International Law.” *The American Journal of International Law* 115 (2): 309–317. https://doi.org/10.1017/ajil.2021.10.

Greenleaf, Graham, and Steven Livingston. 2022. “China’s Personal Information Protection Law: Neither GDPR nor ‘China-style.’” *Privacy Laws & Business International Report* 172: 1–6. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4049445.

Hao, Karen. 2019. “How China Is Using AI in Classrooms—to Track Students’ Focus.” *MIT Technology Review*, August 2, 2019. https://www.technologyreview.com/2019/08/02/133214/how-china-is-using-ai-in-classrooms-to-track-students.

Morley, Jessica, Luciano Floridi, Libby Kinsey, and Anat Elhalal. 2020. *The Ethics of AI in Education: Promises and Perils*. OECD Education Working Paper No. 216. Paris: OECD Publishing. https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=EDU/WKP(2020)14&docLanguage=En.

Sharma, Rakesh. 2021. "Data Governance in Democratic Institutions: Securing the Electoral Process." *Information* 12 (3): 97. https://www.mdpi.com/2078-2489/12/3/97.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.